

Midocean University

College of Informatics

Department of Artificial Intelligence



PROBLEM STATEMENT AND RESEARCH OBJECTIVE FOR CYBERSECURITY AND THREAT DETECTION

Prepared by:

Sultan Khalaf Alotaibi (222000226)

Supervised by:

Dr.Mohammed Anbar

First semester 2025

PROBLEM STATEMENT AND RESEARCH OBJECTIVE FOR CYBERSECURITY AND THREAT DETECTION

Problem Statement

Since cyber threats are constantly changing, there is a great danger to digital infrastructure that calls for sophisticated detection and response systems. Traditional cybersecurity techniques including rule-based systems and signature-based threat detection have difficulty dealing with new developments including zero-day exploits, insider attacks, and advanced phishing tactics. Recent developments in Artificial Intelligence (AI) and Machine Learning (ML) have shown better threat detection using anomaly detection, behavioural analysis, and real-time response automation. Notwithstanding these improvements, existing AI-driven cybersecurity solutions have many significant drawbacks, such as high false positive rates, hostile vulnerabilities, computational overhead, and ethical concerns.

Especially in Internet of Things (IoT) settings and insider threat cases, the literature emphasizes the accuracy of deep learning models; including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs); in identifying cyber dangers. Still, these techniques demand significant computational power, therefore restricting their use in resource-limited settings. Natural Language Processing (NLP)-based threat detection has also shown promise in reducing phishing attacks, but bias in AI training data and model

opacity are still significant problems. Moreover, adversarial machine learning approaches enable threat agents to go around AI security systems, therefore compromising the strength of current cyber security models.

Even with these developments, there is a crucial lack in linking artificial intelligence cyber security systems with current security infrastructure to improve real time threat answer, increase computer efficiency, and guarantee moral openness. Effective real-world applications would call for research to create adaptive, explainable, and computationally efficient AI-driven security systems that can effectively fight cyber risks while also handling adversarial robustness, ethical issues, and deployment problems.

Research Objectives:

This study's main goal is to create an improved AI-based cyber security architecture that improves ethical openness, response automation, and threat detection. The particular objectives are:

- To assess artificial intelligence-based cyber security systems in terms of their capacity to find and stop changing internet threats together with their benefits, constraints, and operational issues.
- To assess the performance of many machine learning approaches; such supervised learning., unsupervised learning., and reinforcement learning; in internet security scenarios.

- To create an AIpowered cybersecurity system that improves live threat identification and meshes effortlessly with current security systems.
- Given artificial intelligence-driven threat detection models, research the moral, openness, and adversarial risks thereof and suggest approaches to improve AI explainability and governance.
- To maximize AI-driven cybersecurity solutions to lower computational overhead and increase scalability, particularly in IoT and cloud settings.

References

- Ismail, W. S. (2024). Threat Detection and Response Using AI and NLP in Cybersecurity. *J. Internet Serv. Inf. Secur.*, 14(1), 195-205. <https://jisis.org/wp-content/uploads/2024/03/2024.I1.013.pdf>
- Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, 21(1), 2286-2295. <https://wjarr.co.in/wjarr-2024-0315>
- Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, 10(5), 055-060. https://www.academia.edu/download/102883869/IJAERS_08_may_2023.pdf
- Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017, February). Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams. In *AAAI Workshops* (pp. 224-231). <https://cdn.aaai.org/ocs/ws/ws0325/15126-68350-2-PB.pdf>
- Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cybersecurity threats detection in internet of things using deep learning approach. *IEEE access*, 7, 124379-124389. <https://ieeexplore.ieee.org/abstract/document/8812669/>

Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity*, 7(12), 25-43.

https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-CYBERSECURITY-Asad-Yaseen.pdf